



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/683,728	10/09/2003	Wei Sun	03226.475001; P8956	1630
32615	7590	01/09/2008		
OSHA LIANG L.L.P./SUN 1221 MCKINNEY, SUITE 2800 HOUSTON, TX 77010			EXAMINER OKORONKWO, CHINWENDU C	
			ART UNIT	PAPER NUMBER
			2136	
			NOTIFICATION DATE	DELIVERY MODE
			01/09/2008	ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

lord@oshaliang.com  
hernandez@oshaliang.com  
DOCKETING@OSHALIANG.COM

## Office Action Summary

Application No.

10/683,728

Applicant(s)

SUN ET AL.

Examiner

Chinwendu C. Okoronkwo

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 06 July 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-28 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-28 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- ☐ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☐ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- ☐ Notice of Informal Patent Application
- ☐ Other: \_\_\_\_\_

**DETAILED ACTION**

***Response to Remarks/Arguments***

1. In response to communications filed on 04/09/2007, applicant amends claims 1, 2, 11, 12, 18 and 19. The following claims, claims 1-26, are presented for examination.

1.1 Applicant's arguments, pages 11-17, with respect to the rejection of claims 1-26 have been fully considered but they are not persuasive.

1.2 The Examiner acknowledges that the previous Office Action listed claims 6, 16 and 23 as being rejected under USC 102 (e), however in actuality these claims were rejected under 103(a).

1.3 In response to Applicant argument that the Cheng reference does not teach or suggest, the generating artifacts that can be used by trusted partner sites to retrieve assertion information to authorize user access from a central service provider, Examiner respectfully disagrees citing column 1 lines 11-35 which clearly recites, "cookies stored in the domain's cookie jar," which are created (generated) "after completion of ... an authentication," therefore the Applicant has not overcome the rejection and the Examiner maintains the rejection.

***Priority***

Art Unit: 2136

2. For the record, the Examiner acknowledges that no priority claim has been made in regards to this application.

***Information Disclosure Statement***

3. For the record, the Examiner acknowledges that no IDS has yet to have been received with this application submitted on 10/09/2003.

***Oath/Declaration***

4. For the record, the Examiner acknowledges that the Oath/Declaration submitted on 10/09/2003 has been received and considered.

***Drawings***

5. For the record, the Examiner acknowledges that the drawings submitted on 07/06/2007 have been received and considered and the objection has been overcome.

***Specification***

6. For the record, the Examiner acknowledges that the Specification submitted on 10/09/2003 has been received and considered.

***Claim Rejections - 35 USC § 102***

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

Art Unit: 2136

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-5, 7-15, 17-22 and 24-26 are rejected under 35 U.S.C. 102(e) as being disclosed by Cheng et al. (U.S. Patent No. 7,010,582 B1).

Regarding claim 1, Cheng et al., discloses a method of performing single sign-on services for a network of trusted partner sites comprising:

- a) generating by a central service provider, assertion information comprising identity information associated with a user that is authorized to sign on to said network, each of said network of trusted partner sites communicatively coupled together through a communication network (col. 2 lines 11-35);
- b) generating by said central service provider, a plurality of artifacts that are associated with said assertion information (col. 1 lines 46-60);
- c) sending, by said central service provider, said plurality of artifacts to a group of trusted partner sites of said network in order to facilitate single sign-on capabilities of said network, wherein each of said group of trusted partner sites can use an artifact of said plurality of artifacts to retrieve said assertion information from said central service provider to individually authorize access by said user. (col. 2 lines 55-67 and col. 3 lines 1-15).

Regarding claim 2, Cheng et al., discloses the method as described in Claim i, wherein said a) further comprises: receiving a sign-on request from said user, retrieving said identity information associated with said user from said central service provider to authenticate said user and authorizing said user access to said network when said user is authenticated (col. 2 lines 11-35).

Regarding claim 3, Cheng et al., discloses the method as described in Claim i, further comprising:

- d) receiving a first artifact of said plurality of artifacts through said communication network from a first trusted partner site, said group of trusted partner sites including said first trusted partner site (col. 3 lines 16-39);
- e) authenticating said first artifact to said first trusted partner site (col. 3 lines 16-39); and
- f) sending said assertion information to said first trusted partner site, transparently to said user, to enable said first trusted partner site to authenticate said user and authorize access to said first trusted partner site by said user (col. 3 lines 40-67).

Regarding claim 4, Cheng et al., discloses the method as described in Claim i, further comprising:

- d) receiving a first artifact of said plurality of artifacts through said communication

network from a first trusted partner sites not from said group of trusted partner sites, wherein said first trusted partner site received said' first artifact from one of said group of trusted partner sites (col. 3 lines 16-39);

e) authenticating said first artifact (col. 3 lines 16-39);

f) sending said assertion information to said first trusted partner site, transparently to said user, to enable said first trusted partner site to authenticate said user and authorize access to said first trusted partner site by said user (col. 3 lines 40-67).

Regarding claim 5, Cheng et al., discloses the method as described in Claim i, further comprising:

d) receiving other assertion information from a first trusted partner site of said network of trusted partner sites, said assertion information comprising data (col. 2 lines 11-35);

e) storing said other assertion information (col. 1 lines 30-36);

f) generating another artifact associated with said other assertion information (col. 1 lines 46-60); and

g) sending said another artifact to a second trusted partner site as directed by said first trusted partner site to facilitate a transfer of said data from said first trusted partner site to said second trusted partner site, wherein said another

Art Unit: 2136

artifact allows access to said other assertion information (col. 2 lines 55-67 and col. 3 lines 1-15).

Regarding claim 7, Cheng et al., discloses the method as described in Claim I, wherein said a) further comprises: sending said plurality of artifacts to a first trusted partner site of said group of trusted partner sites as directed by said user (col. 2 lines 55-67 and col. 3 lines 1-15).

Regarding claim 8, Cheng et al., discloses the method as described in Claim I, wherein said a) further comprises: sending said plurality of artifacts to a first trusted partner site of said group of trusted partner sites as directed by a second trusted partner site of said group of trusted partner sites authorized access to said assertion information (col. 2 lines 55-67 and col. 3 lines 1-15).

Regarding claim 9, Cheng et al., discloses the method as described in Claim I, wherein said c) further comprises: tagging each of said plurality of artifacts for use solely by a corresponding trusted partner site in said group of trusted partner sites (col. 9 lines 37-60).

Regarding claim 10, Cheng et al., discloses the method as described in Claim I, further comprising: d) expiring a first artifact after use of said first artifact by a



trusted partner site to retrieve said assertion information (col. 6 lines 54-67 and col. 7 lines 1-21).

Regarding claim 11, Cheng et al., discloses the method of performing single sign-on services for a network of trusted partner sites comprising:

- a) receiving a first artifact at a first trusted partner site from a central service provider, said central service provider providing single sign-on access to said network of trusted partner sites, said first artifact associated with assertion information comprising identity information associated with a user, said user desiring access to said first trusted partner site, each of said network of trusted partner sites and said central service provider communicatively coupled through a communication network (col. 2 lines 11-35);
- b) sending said first artifact, by said trusted partner site, to said central service provider over said communication network to retrieve said assertion information (col. 1 lines 46-60);
- c) receiving said assertion information from said central service provider at said first trusted partner site over said communication network (col. 2 lines 55-67 and col. 3 lines 1-15); and
- d) determining authorization for said user to access said first trusted partner site based on said assertion information (col. 3 lines 16-39).

Regarding claim 12, Cheng et al., discloses the method as described in Claim ii, further comprising: receiving a second artifact at a second trusted partner site from said central service provider, said user desiring access to said second trusted partner site, said second artifact associated with said assertion information, sending, by said second trusted partner site, said second artifact to said central service provider over said communication network to retrieve said assertion information, receiving said assertion information from said central service provider at said second trusted partner site over said communication network and determining authorization for said user to access said second trusted partner site based on said assertion information (col. 4 lines 60-67 and col. 5 lines 1-15).

Regarding claim 13, Cheng et al., discloses the method as described in Claim 11, wherein said central service provider previously authorizing said user to sign-on to said network of trusted partner sites, said central service provider generating and storing said assertion information (col. 2 lines 11-35).

Regarding claim 14, Cheng et al., discloses the method as described in Claim 11, wherein said a) further comprises: said receiving said first artifact at said first trusted partner site from said central service provider at a direction by a second trusted partner site authorized access to said assertion information (col. 2 lines 11-35).

Regarding claim 15, Cheng et al., discloses the method as described in Claim 11, further comprising sending said first artifact to a second trusted partner site to facilitate access by said user to said second trusted partner site (col. 6 lines 49-64).

Regarding claim 17, Cheng et al., discloses the method as described in Claim ii, further comprising: bypassing said b) and said c) by sending said first artifact to an assertion manager controlling access to said assertion information for internal access to said assertion information when said first trusted partner site is co-located with said central service provider on a web container; and  
f) receiving said assertion information from said assertion manager at said first trusted partner site (col. 5 lines 50-67 and col. 6 lines 1-2).

Regarding claim 18, Cheng et al., discloses a processor, a computer readable memory coupled to said processor and containing program instructions that, when execute, implement a method of performing single sign-on services for a network of trusted partner sites comprising: generating, by a central service provider, assertion information comprising identity information associated with a user that is authorized to sign on to said network, each of said network of trusted partner sites communicatively coupled together through a communication network, generating, by said central service provider a plurality of artifacts that

are associated with said assertion information, sending, by said central service provider, said plurality of artifacts to a group of trusted partner sites of said network in order to facilitate single sign-on capabilities of said network, wherein each of said group of trusted partner sites can use an artifact of said plurality of artifacts to retrieve said assertion information from said central service provider to individually authorize access by said user (Rejected under the same rationale as claim 1 and col. 4 lines 20-27).

Regarding claim 19, Cheng et al., discloses the computer system as described in Claim 18, wherein said a) in said method further comprises:

a) receiving a sign-on request from said user, retrieving said identity information associated with said user from said central service provider to authenticate said user and authorizing said user access to said network when said user is authenticated (Rejected under the same rationale as claim 2 and col. 4 lines 20-27).

Regarding claim 20, Cheng et al., discloses the computer system as described in Claim 18, wherein said method further comprises: d) receiving a first artifact of said plurality of artifacts through said communication from a first trusted partner site, said group of trusted partner sites including said first trusted partner site, e) authenticating said first artifact to said first trusted partner site; and f) sending said assertion information to said first trusted partner site,

transparently to said user to enable said first trusted partner site to authenticate said user and authorize access to said first trusted partner site by said user

(Rejected under the same rationale as claim 3 and col. 4 lines 20-27)

Regarding claim 21, Cheng et al., discloses the computer system as described in Claim 18, wherein said method further comprises: receiving a first artifact of said plurality of artifacts through said communication network from a first trusted partner site not from said group of trusted partner sites, wherein said first trusted partner site received said first artifact from one of said group of trusted partner sites, authenticating said first artifact, authenticating said first artifact; and sending said assertion information to said first trusted partner site, transparently to said user, to enable said first trusted partner site to authenticate said user and authorize access to said first trusted partner site by said user (Rejected under the same rationale as claim 4 and col. 4 lines 20-27).

Regarding claim 22, Cheng et al., discloses the compute system as described in Claim 18, wherein said method further comprises: receiving other assertion information from a first trusted partner site of said network of trusted partner sites, said assertion information comprising data, storing said other assertion information, generating another artifact associated with said other assertion information and sending said another artifact to a second trusted partner site as directed by said first trusted partner site to facilitate a transfer of said data from

said first trusted partner site to said second trusted partner site, wherein said another artifact allows access to said other assertion information (Rejected under the same rationale as claim 5 and col. 4 lines 20-27).

Regarding claim 24, Cheng et al., discloses a computer system as described in Claim 18, wherein said a) in said method further comprises: sending said plurality of artifacts to a first trusted partner site of said group of trusted partner sites as directed by a second trusted partner site of said group of trusted partner sites authorized access to said assertion information (Rejected under the same rationale as claim 1 and col. 4 lines 20-27).

Regarding claim 25, Cheng et al., discloses the computer system as described in Claim 18, wherein said c) in said method further comprises: tagging each of said plurality of artifacts for use solely by a corresponding trusted partner site in said group of trusted partner sites (Rejected under the same rationale as claim 9 and col. 4 lines 20-27).

Regarding claim 26, Cheng et al., discloses the computer system as described in Claim 18, wherein said method further comprises: expiring a first artifact after use of said first artifact by a trusted partner site to retrieve said assertion information (Rejected under the same rationale as claim 10 and col. 4 lines 20-27).

***Claim Rejections - 35 USC § 103***

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 6, 16 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cheng et al. and further in view of Botz et al. (US 2003/0177388 A1).

Cheng et al. is silent in disclosing the method as described in Claim I, wherein said assertion information and said plurality of artifacts substantially comply with a Security Assertions Markup Language (SAML) standard, and said network of trusted partner sites facilitates web browser single sign-on capabilities using interoperational protocols substantially complying with said SAML standard, however Botz et al. does disclose such a method (0066 of Botz et al.).

It would have been obvious for one of ordinary skill in the art, at the time of the invention, to have been motivated to combine the system and method for providing interactions between multiple servers and an end user with the authentication identity translation within a multiple computing unit environment of Botz et al. Cheng hints towards the possible benefit of such a combination in the recitation of the need for a "some standard data format should be agreed

Art Unit: 2136

upon to pass the information from site to site. Furthermore, preferably this passing of confidential information should be done in a secure fashion, by using some sort of cryptographic means for example (col. 11 lines 47-52).” Botz et al. provides motivation for the combination in the description of, “ the emerging web services computing model, [in which] the various AIT logical processes e.g., Domain Controller and interface services could be implemented as published and subscribed to web accessible services. Likewise, ITTs and ITTRs could be stored as published XML documents which could be further implemented using the Security Assertion Markup Language (SAML), which is a proposed standard.” Clearly there is motivation and benefit to modify the invention of Cheng towards compliance with a technology, namely SAML which is a proposed standard.

### ***Conclusion***

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of



Art Unit: 2136

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chinwendu C. Okoronkwo whose telephone number is (571) 272 2662. The examiner can normally be reached on MWF 2:30 - 6:00, TR 9:00-3:30.

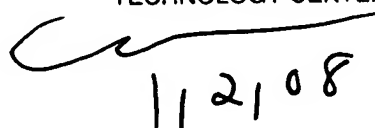
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272 4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

  
Nasser Moazzami

December 31, 2007

NASSER MOAZZAMI  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

  
11/21/08